IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (Currently Amended) An information processing method ~~in~~ executed by a center system, said information processing method comprising:

receiving a first digital signature for specific data stored in said center system and a request to allow ~~data concerning~~ a first user to ~~be allowed to~~ read said stored specific data, from a terminal of a second user;

confirming if an authority to give said first user permission to read said stored specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

if said first signature and said second signature are identical, performing a processing for enabling said first user to read said stored specific data.

2. (Currently Amended) The information processing method as set forth in claim 1, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represents that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

3. (Currently Amended) The information processing method as set forth in claim 1, further comprising:

if said first signature and said second signature are not identical, generating second hash data from said first digital signature;

confirming if said authority to give said first user said permission to read said stored specific data is granted to said second user by comparing the generated second hash data with

hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

executing a processing for enabling said first user to read said stored specific data.

4. (Currently Amended) The information processing method as set forth in claim 3, wherein said executing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represent that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

5. (Currently Amended) An access authority management method ~~in~~ executed by a center system, said access authority management method comprising:

receiving a first digital signature for specific data stored in said center system from a terminal of a user;

confirming if an authority to update said stored specific data is granted to said user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

if said first digital signature and said second digital signature are identical, carrying out a setting to allow said user to update said stored specific data.

6. (Currently Amended) The access authority management method as set forth in claim 5, further comprising:

if said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature;

confirming if an authority to read said stored specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

if said first hash data and said second hash data are identical, carrying out a setting to allow said user to read said stored specific data.

7. (previously presented) The access authority management method as set forth in claim 6, further comprising transmitting an access denial notice to said terminal of said user, if said first hash data and said second hash data are not identical.

8. (Currently Amended) The access authority management method as set forth in claim 5, further comprising:

if data for updating said stored specific data is received from said terminal of said user, generating third hash data for the updated specific data;

transmitting said third hash data to said terminal of said user; receiving a third digital signature generated from said third hash data, from said terminal of said user; and

registering said updated stored specific data, said third hash data, and said third digital signature into said data storage unit.

9. (previously presented) The access authority management method as set forth in claim 8, further comprising:

generating fourth hash data from said third digital signature before said registering; and

comparing said fourth hash data with said third hash data, and wherein said registering is executed if said fourth hash data and said third hash data are identical.

10. (Currently Amended) The access authority management method as set forth in claim 6, further comprising, if said authority to read said stored specific data is granted to said user, transmitting said stored specific data in a state where only reading is enabled, to said terminal of said user.

11. (Currently Amended) A data registration method ~~in~~ executed by a center system, said data registration method comprising:

if specific data is received by said center system from a user terminal, ~~generate~~ generating hash data for said specific data;

transmitting said hash data to said user terminal;

receiving a digital signature generated from said hash data from said user terminal; and

registering said specific data, said hash data and said digital signature into a data storage unit, ~~and~~

wherein the registered hash and the registered digital signature are used to confirm if an authority to access said specific data is granted to an access requestor.

12. (previously presented) A data access method in a user system, comprising:

generating a digital signature from hash data, which is stored in a hash storage, for specific data;

transmitting an access request including said digital signature as data representing permission to update said specific data to a server; and

if said digital signature and a second digital signature, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where updating is enabled, from said server.

13. (previously presented) The data access method as set forth in claim 12, further comprising, if said digital signature and said second digital signature, which is registered in said server, for said specific data are not identical, but hash data, which represents that an authority to read said specific data is granted to said user, and which is generated from said digital signature, and second hash data, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where only reading is enabled, from said server.

14. (Currently Amended) A computer-readable medium storing a program ~~for~~ causing an apparatus to ~~execute~~perform operations comprising:

receiving a first digital signature for specific data stored in said apparatus and ~~data concerning~~a request to allow a first user ~~to be allowed~~ to read said stored specific data, from a terminal of a second user;

confirming if an authority to give said first user permission to read said stored specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

if said first signature and said second signature are identical, performing a processing for enabling said first user to read said stored specific data.

15. (Currently Amended) The computer-readable medium as set forth in claim 14, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represents that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

16. (Currently Amended) The computer-readable medium as set forth in claim 14, further comprising:

if said first signature and said second signature are not identical, generating second hash data from said first digital signature;

confirming if said authority to give said first user said permission to read said stored specific data is granted to said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

executing a processing for enabling said first user to read said stored specific data.

17. (Currently Amended) The computer-readable medium as set forth in claim 16, wherein said executing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represents that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

18. (Currently Amended) A computer-readable medium storing a program ~~for~~causing an apparatus managing ~~an~~ access authority ~~management, said program causing an apparatus to~~ by performing operations comprising~~execute~~:

receiving a first digital signature for specific data stored in said apparatus from a terminal of a user;

confirming if an authority to update said stored specific data is granted to said user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

if said first digital signature and said second digital signature are identical, carrying out a setting to allow said user to update said stored specific data.

19. (Currently Amended) The computer-readable medium as set forth in claim 18, further comprising:

if said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature;

confirming if an authority to read said stored specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

if said first hash data and said second hash data are identical, carrying out a setting to allow said user to read said stored specific data.

20. (previously presented) The computer-readable medium as set forth in claim 19, further comprising transmitting an access denial notice to said terminal of said user, if said first hash data and said second hash data are not identical.

21. (Currently Amended) The computer-readable medium as set forth in claim 18, further comprising:

if data for updating said stored specific data is received from said terminal of said user, generating third hash data for the updated specific data;

transmitting said third hash data to said terminal of said user;

receiving a third digital signature generated from said third hash data, from said terminal of said user; and

registering said updated stored specific data, said third hash data, and said third digital signature into said data storage unit.

22. (previously presented) The computer-readable medium as set forth in claim 21, further comprising:

generating fourth hash data from said third digital signature before said registering; and

comparing said fourth hash data with said third hash data, and wherein said registering is executed if said fourth hash data and said third hash data are identical.

23. (Currently Amended) The computer-readable medium as set forth in claim 19, further comprising, if said authority to read said stored specific data is granted to said user, transmitting said stored specific data in a state where only reading is enabled, to said terminal of said user.

24. (Currently Amended) A center system, comprising:

a unit that receives a first digital signature for specific data stored in said center system and ~~data concerning~~ a request to allow a first user ~~to be allowed~~ to read said stored specific data, from a terminal of a second user;

a unit that confirms if an authority to give said first user permission to read said stored specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

a unit that performs a processing enabling said first user to read said stored specific data, if said first signature and said second signature are identical.

25. (Currently Amended) The center system as set forth in claim 24, wherein said unit that performs a processing comprises a unit that transmits hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represents that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

26. (Currently Amended) The center system as set forth in claim 24, further comprising:

a unit that generates second hash data from said first digital signature, if said first signature and said second signature are not identical;

a unit that confirms if said authority to give said first user said permission to read said stored specific data is granted to said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

a unit that executes a processing enabling said first user to read said stored specific data.

27. (Currently Amended) The center system as set forth in claim 26, wherein said unit that executes a processing comprises a unit that transmits hash data, which is registered in said data storage unit so as to correspond to said stored specific data, and which represents that an authority to read said stored specific data is granted to said first user, to a terminal of said first user.

28. (Currently Amended) A center system, comprising:

a unit that receives a first digital signature for specific data stored in said center system from a terminal of a user;

a unit that confirms if an authority to update said stored specific data is granted to said user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and

a unit that carries out a setting to allow said user to update said stored specific data, if said first digital signature and said second digital signature are identical.

29. (Currently Amended) The center system as set forth in claim 28, further comprising:

a unit that generates a first hash data from said first digital signature, if said first digital signature and said second digital signature are not identical;

a unit that confirms if an authority to read said stored specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said stored specific data; and

a unit that carries out a setting to allow said user to read said stored specific data, if said first hash data and said second hash data are identical.

30. (previously presented) The center system as set forth in claim 29, further comprising a unit that transmitting an access denial notice to said terminal of said user, if said first hash data and said second hash data are not identical.

31. (Currently Amended) The center system as set forth in claim 28, further comprising:

a unit that generates, if data for updating said stored specific data is received from said terminal of said user, third hash data for the updated specific data;

a unit that transmits said third hash data to said terminal of said user;

a unit that receives a third digital signature generated from said third hash data, from said terminal of said user; and

a unit that registers said updated stored specific data, said third hash data, and said third digital signature into said data storage unit.

32. (previously presented) The center system as set forth in claim 31, further comprising:

a unit that generates a fourth hash data from said third digital signature before said registering; and

a unit that compares said fourth hash data with said third hash data, and wherein said unit that registers operates if said fourth hash data and said third hash data are identical.

33. (Currently Amended) The center system as set forth in claim 29, further comprising a unit that transmits said stored specific data in a state where only reading is

enabled, to said terminal of said user, if said authority to read said stored specific data is granted to said user.